Installation d'un module SFR sur un module matériel ASA 5585-X

Contenu

Introduction

Le module ASA FirePOWER, également appelé ASA SFR, fournit des services de pare-feu de nouvelle génération, notamment les systèmes de prévention des intrusions de nouvelle génération (NGIPS), la visibilité et le contrôle des applications (AVC), le filtrage des URL et la protection avancée contre les programmes malveillants (AMP). Vous pouvez utiliser le module en mode de contexte simple ou multiple, et en mode routé ou transparent. Ce document décrit les conditions préalables et les processus d'installation d'un module FirePOWER (SFR) sur le module matériel ASA 5585-X. Il fournit également les étapes pour enregistrer un module SFR avec FireSIGHT Management Center.

> **Note**: Les fonctionnalités FirePOWER (SFR) résident sur un module matériel de la gamme ASA 5585-X, tandis que les services FirePOWER des gammes ASA 5512-X à 5555-X sont installés sur un module logiciel, ce qui entraîne des différences dans les processus d'installation.

Conditions préalables

Conditions requises

Les instructions de ce document nécessitent un accès au mode d’exécution privilégié. Pour accéder au mode d’exécution privilégié, entrez la commande enable. Si aucun mot de passe n'a été défini, il suffit de cliquer sur Entrée.

```
ciscoasa> enable
Password:
ciscoasa#
```

Pour installer FirePOWER Services sur un ASA, les composants suivants sont nécessaires :

- Logiciel ASA version 9.2.2 ou ultérieure
- Plate-forme ASA 5585-X
- Un serveur TFTP accessible par l'interface de gestion du module FirePOWER
- FireSIGHT Management Center avec version 5.3.1 ou ultérieure

> **Note**: Les informations de ce document sont créées à partir des périphériques d'un environnement de travaux pratiques spécifique. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Avant de commencer

Étant donné qu'un module ASA SSM occupe toujours l'un des deux logements du châssis ASA 5585-X, si vous avez un module matériel autre que le SSP FirePOWER (SFR) Services, tel que le SSP-CX (Context Aware) ou AIP-SSM (Advanced Inspection and Prevention Security), l'autre module doit être désinstallé pour libérer de l'espace pour le SSP-SFR. Avant de retirer un module matériel, exécutez la commande suivante pour arrêter un module :

```
ciscoasa# hw-module module 1 shutdown
```

Câblage et gestion

- Vous ne pouvez pas accéder au port série du module SFR via la console ASA sur l'ASA 5585-X.
- Une fois le module SFR provisionné, vous pouvez vous connecter à la lame à l'aide de la commande session 1.
- Afin de réinstaller complètement le module SFR sur un ASA 5585-X, vous devez utiliser l'interface Ethernet de gestion et une session de console sur le port de gestion série, qui se trouvent sur le module SFR et sont séparés de l'interface de gestion et de la console ASA.

> **Astuce** : Afin de trouver l'état d'un module sur l'ASA, exécutez la commande show module 1 details" qui récupère l'adresse IP de gestion du module SFR et le Centre de défense associé.

Installation du module FirePOWER (SFR) sur ASA

1. Téléchargez l'image de démarrage initiale du module ASA FirePOWER SFR depuis Cisco.com vers un serveur TFTP accessible depuis l'interface de gestion ASA FirePOWER. Le nom de l'image ressemble à "asasasfr-boot-5.3.1-152.img"

2. Téléchargez le logiciel système ASA FirePOWER depuis Cisco.com vers un serveur HTTP, HTTPS ou FTP accessible depuis l'interface de gestion ASA FirePOWER.

3. Redémarrer le module SFR

Option 1 : Si vous n'avez pas le mot de passe du module SFR, vous pouvez émettre la commande suivante à partir de l'ASA pour redémarrer le module.

```
ciscoasa# hw-module module 1 reload
Reload module 1? [confirm]
Reload issued for module 1
```

Option 2 : Si vous avez le mot de passe du module SFR, vous pouvez redémarrer le capteur directement à partir de sa ligne de commande.

```
Sourcefire3D login: admin
Password:

Sourcefire Linux OS v5.3.1 (build 43)
Sourcefire ASA5585-SSP-10 v5.3.1 (build 152)

>system reboot
```

4. Interrompez le processus de démarrage du module SFR à l'aide d'ESCAPE ou de la séquence d'interruption de votre logiciel de session de terminal pour placer le module dans ROMMON.

```
The system is restarting...
CISCO SYSTEMS
Embedded BIOS Version 2.0(14)1 15:16:31 01/25/14



Cisco Systems ROMMON Version (2.0(14)1) #0: Sat Jan 25 16:44:38 CST 2014

Platform ASA 5585-X FirePOWER SSP-10, 8GE

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in 8 seconds.

Boot interrupted.

Management0/0
Link is UP
MAC Address: xxxx.xxxx.xxxx
```

```
Use ? for help.

rommon #0>
```

5. Configurez l'interface de gestion de module SFR avec une adresse IP et indiquez l'emplacement du serveur TFTP et du chemin TFTP vers l'image de démarrage. Entrez les commandes suivantes pour définir une adresse IP sur l'interface et récupérer l'image TFTP :

- `set`
- ADDRESS = Votre_adresse_IP
- GATEWAY = Votre_Passerelle
- SERVER = Votre_serveur_TFTP
- IMAGE = Your_TFTP_Filepath
- `synchroniser`
- `tftp`

! Exemple d'informations d'adresse IP utilisées. Mise à jour pour votre environnement.

```
rommon #1> ADDRESS=198.51.100.3
rommon #2> GATEWAY=198.51.100.1
rommon #3> SERVER=198.51.100.100
rommon #4> IMAGE=/tftpboot/asasfr-boot-5.3.1-152.img
rommon #5> sync

Updating NVRAM Parameters...

rommon #6> tftp
ROMMON Variable Settings:
ADDRESS=198.51.100.3
SERVER=198.51.100.100
GATEWAY=198.51.100.1
PORT=Management0/0
VLAN=untagged
IMAGE=/tftpboot/asasfr-boot-5.3.1-152.img
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20

tftp /tftpboot/asasfr-boot-5.3.1-152.img@198.51.100.100 via 198.51.100.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<truncated output>

Received 41235627 bytes

Launching TFTP Image...

Execute image at 0x14000
```

6. Connectez-vous à l'image de démarrage initiale. Connectez-vous en tant qu'administrateur et avec le mot de passe Admin123

```
Cisco ASA SFR Boot Image 5.3.1
```

```
asasfr login: admin
Password:

Cisco ASA SFR Boot 5.3.1 (152)
Type ? for list of commands
```

7. Utilisez l'image de démarrage initiale pour configurer une adresse IP sur l'interface de gestion du module. Entrez la commande setup pour accéder à l'assistant. Vous êtes invité à fournir les informations suivantes :

- **Nom de l'hôte:** Jusqu'à 65 caractères alphanumériques, sans espace. Les tirets sont autorisés.
- **Adresse réseau** : Vous pouvez définir des adresses IPv4 ou IPv6 statiques, ou utiliser DHCP (pour IPv4) ou la configuration automatique sans état IPv6.
- **Informations DNS** : Vous devez identifier au moins un serveur DNS et vous pouvez également définir le nom de domaine et le domaine de recherche.
- **Informations NTP** : Vous pouvez activer NTP et configurer les serveurs NTP, pour définir l'heure système.

! Exemple d'informations utilisées. Mise à jour pour votre environnement.

```
asasfr-boot>setup

Welcome to SFR Setup
[hit Ctrl-C to abort]
Default values are inside []

Enter a hostname [asasfr]: sfr-module-5585
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address on management interface?(y/n) [N]: N
Enter an IPv4 address [192.168.8.8]: 198.51.100.3
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 198.51.100.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: N
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address: 198.51.100.15
Do you want to configure Secondary DNS Server? (y/n) [n]: N
Do you want to configure Local Domain Name? (y/n) [n]: N
Do you want to configure Search domains? (y/n) [n]: N
Do you want to enable the NTP service? [Y]: N

Please review the final configuration:
Hostname: sfr-module-5585
Management Interface Configuration

IPv4 Configuration: static
IP Address: 198.51.100.3
Netmask: 255.255.255.0
Gateway: 198.51.100.1

IPv6 Configuration: Stateless autoconfiguration

DNS Configuration:
DNS Server: 198.51.100.15

Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
```

```
Restarting network services...
Restarting NTP service...
Done.
```

8. Utilisez l'image de démarrage pour extraire et installer l'image du logiciel système à l'aide de la commande **system install**. Incluez l'option **noconfirm** si vous ne voulez pas répondre aux messages de confirmation. Remplacez le mot clé *url* par l'emplacement du fichier .pkg.

```
asasfr-boot> system install [noconfirm] url
```

Exemple :

```
> system install http://Server_IP_Address/asasfr-sys-5.3.1-152.pkg

Verifying
Downloading
Extracting

Package Detail
Description: Cisco ASA-SFR 5.3.1-152 System Install
Requires reboot: Yes

Do you want to continue with upgrade? [y]: Y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image ...
```

> **Note**: Une fois l'installation terminée dans 20 à 30 minutes, vous serez invité à appuyer sur la touche Entrée pour redémarrer. Comptez 10 minutes ou plus pour l'installation des composants d'application et le démarrage des services ASA FirePOWER. Le résultat de la commande show module 1 details doit afficher tous les processus comme étant Actifs.

État du module pendant l'installation

```
ciscoasa# show module 1 details

Getting details from the Service Module, please wait...
Unable to read details from module 1

Card Type: ASA 5585-X FirePOWER SSP-10, 8GE
Model: ASA5585-SSP-SFR10
Hardware version: 1.0
Serial Number: JAD18400028
Firmware version: 2.0(14)1
Software version: 5.3.1-152
MAC Address Range: 58f3.9ca0.1190 to 58f3.9ca0.119b
App. name: ASA FirePOWER
App. Status: Not Applicable
App. Status Desc: Not Applicable
App. version: 5.3.1-152
Data Plane Status: Not Applicable
Console session: Not ready
Status: Unresponsive
```

État du module après une installation réussie

```
ciscoasa# show module 1 details

Getting details from the Service Module, please wait...

Card Type: ASA 5585-X FirePOWER SSP-10, 8GE
Model: ASA5585-SSP-SFR10
Hardware version: 1.0
Serial Number: JAD18400028
Firmware version: 2.0(14)1
Software version: 5.3.1-152
MAC Address Range: 58f3.9ca0.1190 to 58f3.9ca0.119b
App. name: ASA FirePOWER
App. Status: Up
App. Status Desc: Normal Operation
App. version: 5.3.1-152
Data Plane Status: Up
Console session: Ready
Status: Up
DC addr: No DC Configured
Mgmt IP addr: 192.168.45.45
Mgmt Network mask: 255.255.255.0
Mgmt Gateway: 0.0.0.0
Mgmt web ports: 443
Mgmt TLS enabled: true
```

Configuration

Configurer le logiciel FirePOWER

1.Vous pouvez vous connecter au module FirePOWER ASA 5585-X via l'un des ports externes suivants :

- Port de console ASA FirePOWER
- Interface ASA FirePOWER Management 1/0 avec SSH

  Note: Vous ne pouvez pas accéder à l'interface de ligne de commande du module matériel ASA FirePOWER sur le fond de panier ASA à l'aide de la commande session sfr.

2. Après avoir accédé au module FirePOWER via la console, connectez-vous avec le nom d'utilisateur **admin** et le mot de passe **Sourcefire**.

```
Sourcefire3D login: admin
Password:

Last login: Fri Jan 30 14:00:51 UTC 2015 on ttyS0

Copyright 2001-2013, Sourcefire, Inc. All rights reserved. Sourcefire is a registered
trademark of Sourcefire, Inc. All other trademarks are property of their respective
owners.
```

```
Sourcefire Linux OS v5.3.1 (build 43)
Sourcefire ASA5585-SSP-10 v5.3.1 (build 152)

Last login: Wed Feb 18 14:22:19 on ttyS0

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: dhcp
If your networking information has changed, you will need to reconnect.
[1640209.830367] ADDRCONF(NETDEV_UP): eth0: link is not ready
[1640212.873978] e1000e: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[1640212.966250] ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
For HTTP Proxy configuration, run 'configure network http-proxy'

This sensor must be managed by a Defense Center.  A unique alphanumeric registration
key is always required.  In most cases, to register a sensor to a Defense Center,
you must provide the hostname or the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Defense Center are separated by a NAT device, you
must enter a unique NAT ID, along with the unique registration key. 'configure
manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.

>
```

Configurer FireSIGHT Management Center

Pour gérer un module ASA FirePOWER et une stratégie de sécurité, vous **devez** l'enregistrer auprès d'un FireSIGHT Management Center. Vous ne pouvez pas effectuer les opérations suivantes avec FireSIGHT Management Center :

- Impossible de configurer les interfaces ASA FirePOWER.
- Impossible d'arrêter, de redémarrer ou de gérer les processus ASA FirePOWER.
- Impossible de créer des sauvegardes à partir des périphériques ASA FirePOWER ou de les restaurer.
- Impossible d'écrire les règles de contrôle d'accès pour correspondre au trafic à l'aide des conditions de balise VLAN.

Rediriger le trafic vers le module SFR

Vous redirigez le trafic vers le module ASA FirePOWER en créant une stratégie de service qui identifie le trafic spécifique. Afin de rediriger le trafic vers un module FirePOWER, procédez comme suit :

Étape 1 : Sélectionner le trafic

Tout d'abord, sélectionnez le trafic à l'aide de la commande access-list. Dans l'exemple suivant, nous redirigeons tout le trafic de toutes les interfaces. Vous pouvez également le faire pour un

trafic spécifique.

```
ciscoasa(config)# access-list sfr_redirect extended permit ip any any
```

Étape 2 : Correspondance du trafic

L'exemple suivant montre comment créer une carte-classe et faire correspondre le trafic sur une liste d'accès :

```
ciscoasa(config)# class-map sfr
ciscoasa(config-cmap)# match access-list sfr_redirect
```

Étape 3 : Spécifier l'action

Vous pouvez configurer votre périphérique dans un déploiement passif (« surveillance uniquement ») ou en ligne. Vous ne pouvez pas configurer à la fois le mode surveillance seule et le mode en ligne normal en même temps sur l'ASA. Un seul type de stratégie de sécurité est autorisé.

Mode Inline

Dans un déploiement en ligne, après avoir abandonné le trafic indésirable et pris toute autre action appliquée par la stratégie, le trafic est renvoyé à l'ASA pour traitement ultérieur et transmission finale. L'exemple suivant montre comment créer une carte de stratégie et configurer le module FirePOWER en mode Inline :

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class sfr
ciscoasa(config-pmap-c)# sfr fail-open
```

Mode passif

Dans un déploiement passif,

- Une copie du trafic est envoyée au périphérique, mais elle n'est pas renvoyée à l'ASA.
- Le mode passif vous permet de voir ce que le périphérique aurait fait au trafic et vous permet d'évaluer le contenu du trafic, sans affecter le réseau.

Si vous souhaitez configurer le module FirePOWER en mode passif, utilisez le mot clé monitor-only comme ci-dessous. Si vous n'incluez pas le mot clé, le trafic est envoyé en mode en ligne.

```
ciscoasa(config-pmap-c)# sfr fail-open monitor-only
```

Étape 4 : Spécifier l'emplacement

La dernière étape consiste à appliquer la stratégie. Vous pouvez appliquer une stratégie globalement ou sur une interface. Vous pouvez remplacer la stratégie globale sur une interface en appliquant une stratégie de service à cette interface.

Le mot clé global applique la carte de stratégie à toutes les interfaces et interface applique la stratégie à une interface. Une seule politique globale est autorisée. Dans l'exemple suivant, la stratégie est appliquée globalement :

```
ciscoasa(config)# service-policy global_policy global
```

> **Attention** : La carte de stratégie global_policy est une stratégie par défaut. Si vous utilisez cette stratégie et souhaitez la supprimer sur votre périphérique à des fins de dépannage, assurez-vous de bien comprendre son implication.

Document connexe

- Enregistrer un périphérique avec FireSIGHT Management Center
- Déploiement de FireSIGHT Management Center sur VMware ESXi
- Scénarios de configuration de la gestion IPS sur un module IPS 5500-X